PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-039840
(43)Date of publication of application : 08.02.2000

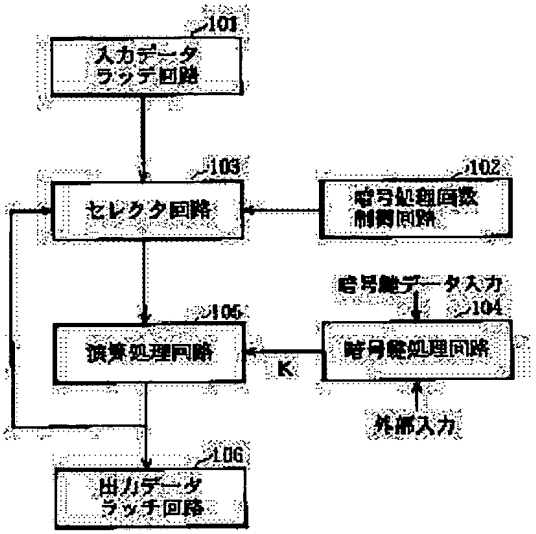
(51)Int.Cl. G09C 1/00
H04L 9/06

(21)Application number : 10-209470
(22)Date of filing : 24.07.1998

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : ANDO YUJI

(54) CIPHER APPARATUS

(57)Abstract:
PROBLEM TO BE SOLVED: To improve the resistance to the eavesdropping, manipulation, etc., by a third person and to enable dealing with the change of a cipher algorithm even in the case of the cryptoanalysis of the algorithm by the third person by creating the cipher key to be used by a data processing means is accordance with previously held data or program for cipher key formation or separate information.
SOLUTION: An arithmetic processing circuit 105 executes arithmetic processing of exclusive OR and various other kinds by using the cipher key made secret for at least the third person (via the reliable third person in some cases) in order to encipher individual pieces of divided data. A cipher key processing circuit 104 creates the cipher key to be used by this arithmetic procreating circuit 105 by use of the previously held data for forming cipher key, for example, a shared key or the secret key (intrinsic 'key') secretly held only on the transmission side or a program for fetching, etc., of only the specific number of digits of the secret key or the use of the secret key in accordance with the separate information on date, etc., from a clock or calendar, etc.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁(JP)　(12)公開特許公報（A）　(11)特許出願公開番号

特開２０００－３９８４０
(P２０００－３９８４０A)
(43)公開日　平成12年2月8日(2000.2.8)

(51)Int.Cl.⁷		識別記号	FI			テーマコード(参考)
G09C	1/00	610	G09C	1/00	610 A	5K013
					610 B	
H04L	9/06		H04L	9/00	611 Z	

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願平10-209470

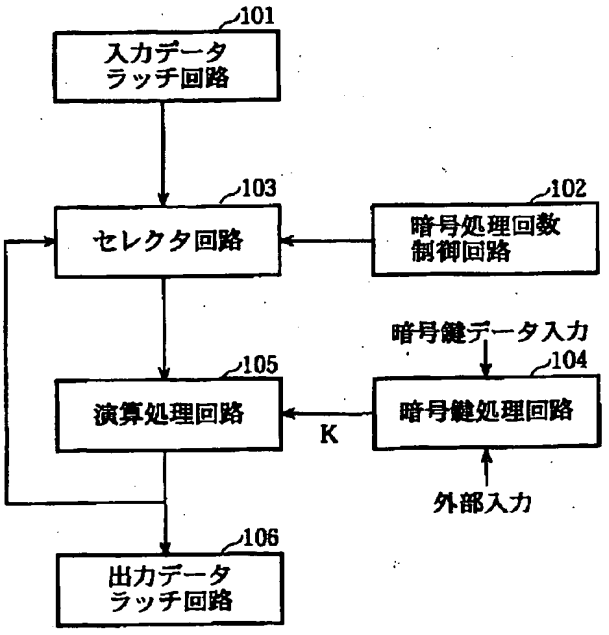
(22)出願日　平成10年7月24日(1998.7.24)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　安藤　裕治
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100101823
弁理士　大前　要

Ｆターム(参考)　5K013 BA02 CA00 EA04

(54)【発明の名称】暗号装置

(57)【要約】
【課題】　インターネットのようなオープンネットワークにおけるディジタルデータ転送に用いられる暗号装置を、既存の暗号装置との互換性を保持しつつ、第三者による盗聴等の攻撃に対する耐性を高め、その信頼性を向上させる。
【解決手段】　仕様変更を行うことなく、暗号アルゴリズムを変更可能にする。具体的には、入力された平文データを暗号鍵と所定の関数に基づいて処理することにより暗号化する演算処理回路で暗号化に用いる鍵を外部入力等に基づいて各平文データやそのブロックデータ毎に変更可能とする。



1

【特許請求の範囲】

【請求項１】　平文を所定のビット数に分割し、得られた個々の分割データを暗号化して送信する暗号装置において、

上記個々の分割データを暗号化するために暗号鍵を使用して演算処理を行うデータ処理手段と、

該データ処理手段が使用する暗号鍵を、予め保持している暗号鍵作成用のデータやプログラムあるいは別途の情報を基に作り出す暗号鍵処理手段とを有していることを特徴とする暗号装置。

【請求項２】　前記データ処理手段は、

前記暗号鍵処理手段から入力された暗号鍵を基に、上記個々の分割データに順に演算処理をする鍵基演算小手段を有していることを特徴とする請求項１記載の暗号装置。

【請求項３】　前記データ処理手段は、

入力された個々の分割データに多段に演算処理を施すが、この際先の段へ入力されたデータの半数が続行する後の段へその半数分の入力データとしてビット桁の位置のみを換えて入力され、先の段から出力されたデータの半数が後の段へその残り半数分の入力データとして入力される演算を行なうインボリューション演算モード小手段を有していることを特徴とする請求項２記載の暗号装置。

【請求項４】　前記鍵基演算小手段は、

各段の演算処理毎に、前記暗号鍵処理手段から異なる暗号鍵を入力されて演算処理をする相違暗号鍵使用小小手段を有していることを特徴とする請求項３記載の暗号装置。

【請求項５】　前記暗号鍵処理手段は、

外部からのデータに基づいて、前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する外部値依存出力小手段を有していることを特徴とする請求項４記載の暗号装置。

【請求項６】　乱数発生手段を有し、

更に前記暗号鍵処理小手段は、

前記乱数発生手段の発生させる乱数にもとづいて、前記データ処理手段に出力する暗号鍵を上記分割データ毎に変更する乱数依存出力小手段を有していることを特徴とする請求項４記載の暗号装置。

【請求項７】　前記暗号鍵処理手段は、

入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更するビット依存出力小手段を有していることを特徴とする請求項４記載の暗号装置。

【請求項８】　前記暗号鍵処理手段は、

前入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する前ビット依存出力小手段を有していることを特徴とする請求項４記載の暗号装置。

2

【請求項９】　前記暗号鍵処理手段は、

前暗号データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する前暗号データ依存鍵変更小手段を有していることを特徴とする請求項４記載の暗号装置。

【発明の詳細な説明】

【０００１】

【発明の所属する技術分野】本発明は暗号装置に関し、特に大量のディジタルデータを暗号化、復号するための装置に関する。

【０００２】

【従来の技術】近年、ＮＴＴ等によるディジタル通信網の整備、衛星からのディジタル映像、音声放送等我が国においても公開通信網によるディジタル送受信が広く利用されるようになってきている。ところで、これらの公開通信網においては、通信を媒介する回線、電波等は秘密に保持しえないため、第三者による盗聴、詐称、無料視聴等を完全に防止するのは困難である。その対策として、通信（送信）文や映像データを暗号化することが広く行なわれている。

【０００３】具体的に簡単な例をあげると、送信者と受信者とであらかじめ暗号化と復号（正当者による解読）に使用する鍵（暗号鍵）といわれる数値を予め定めておき、送信者は送信する文とこの鍵の排他的論理和をとって暗号化した文を送り、受信者は受信文と鍵の排他的論理和をとって復号（解読）を行なうようなものである。

【０００４】この暗号化と復号の具体例を挙げると、ディジタル化された送信文が（１、０、０、１）であり鍵が〔０、１、１、１〕であるならば、両者の排他的論理和で暗号化された送信文は「１、０、０、０」となる。一方、受信したこの送信文と前述の鍵の排他的論理和で復号された文は、元の（１、０、０、１）となる。

【０００５】そして、この鍵の作成方法、配布方法、相手方への何らかの手段による鍵そのものや鍵についての情報の秘密送受信方法等については、種々の発明がなされている。（なお、有料放送においては、鍵を組み込んだＩＣカードを受像機に装着したりすることもなされる。）

【０００６】また、送信文と鍵との演算も排他的論理和を中心に、インボリューション、繰り返し等種々の発明がなされている。（なお、ここで排他的論理和を演算の中心とするのは、送信側と受信側とで機器、ハードを共通にし得ることが多いことによる。）

【０００７】但し、これらのことや鍵についての数学的理論等は、例えば、岡本英治著「暗号理論入門」共栄出版Ｋ．Ｋ．刊、Ｎ．コブリッツ著、櫻井幸一訳「数論アルゴリズムと楕円暗号理論入門」シュプリンガー・フェアラーク・東京、池野信一、小山謙二著「現代暗号理論」電子通信学会刊等に記載されている周知技術である。このため、これらについての一般的な説明は省略す

る。

【０００８】以下、本発明に関係の深い事項に限定して従来の技術を説明する。従来からのデータの暗号方式として対称暗号方式がある。対称暗号方式とは、平文を暗号化するのに用いられる数値たる暗号鍵と、その暗号文を復号するのに用いられる数値たる復号鍵が同じ値（一般に、この数値は「共有鍵」と言われる。）である暗号方式である。

【０００９】この対称暗号方式として有名なものにＤＥＳ（「ディーイーエス」と発音される。）暗号方式がある。ＤＥＳ（Ｄａｔｅ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）暗号方式は、アメリカ商務省標準局（ＮＢＳ：Ｎａｔｉｏｎａｌ　Ｂｕｒｅａｕ　Ｓｔａｎｄａｒｄ　Ｔｅｃｎｏｌｏｇｙ，現ＮＩＳＴ：Ｎａｔｉｏｎａｌ　Ｉｎｓｔｉｔｕｔｅ　ｏｆ　Ｓｔａｎｄａｒｄ　Ｔｅｃｎｏｌｏｇｙ）が１９７７年1月１５日に定めた標準であり、現在もっとも多く用いられているものである。

【００１０】図６に、このＤＥＳ暗号方式により処理を行う際のデータの流れを中心とする回路の構成を示す。このＤＥＳ暗号方式では、通信文が６４ビットずつに区切られ、この区切られた各６４ビットずつの平文が図示の回路に逐次入力され、各入力された平文がこれまた６４ビットずつの暗号文に変換されて出力されるものである。なお、この処理では、暗号鍵も平文入力と同様に６４ビットの数値であるが、そのうち８ビットをパリティ（奇遇検査）に使っているので、暗号鍵は実質５６ビットである。

【００１１】本図において、１０はＤＥＳ方式により暗号化処理を行う回路であり、６４ビット平文入力Ｈｉｎに対して初期転値（ＩＰ処理）を施す初期転値処理部１０ａと、該初期転値処理部から出力されたデータに対して鍵を使用して本来の暗号化の処理を行なう１６段からなる演算処理部１０ｂと、演算処理部から出力されたデータに対して最終転値（ＩＰ－１処理）を施して６４ビットの最終的に暗号化された文Ａｏｕｔを出力する最終転値処理部１０ｃとを有している。

【００１２】ここで、上記転値処理部１０ａは、６４ビット平文入力Ｈｉｎにおけるデータの配列を変える初期転値処理を、転値データに基づいて行う。図５の（ａ）に、この初期転値処理を行うためのデータの表（初期転値表）を示す。この初期転値表は、６４ビットで入力された平文の各ビット（桁）のデータ（桁）が、初期転値を施した６４ビットの出力文の何ビット目のデータになるかを示すものである。

【００１３】具体的には、図５の（ａ）に示す初期転値表における行は、６４ビット平文入力のＬＳＢ（最小位ビット）から数えたバイト位置を示しており、列は６４ビット平文入力のバイト内でのＬＳＢ（最小位ビット）から数えたビット位置を示している。このため、行及び列の交差部に対応する数字が、初期転値処理部からの初期転値出力におけるビット位置を示すことになる。

【００１４】本図において、例えば入力信号のＬＳＢの１ビット目は、１バイト目の１ビット目であるので、上記初期転値表における１行１列目の値の５８より、出力信号の５８ビット目に変換される。また、入力信号の３０ビット目のデータは、４バイト目の６ビットであるので、上記初期転値表における４行６列目の値の２４により、出力信号の２４ビット目に変換される。さらに、信号の６４ビット目は８バイト目の８ビット目であるので、上記初期転値表における８行８列目の値の７により、出力信号の７ビット目に変換される。以上の変換を入力信号の６４ビット全てに対して行うことにより、出力信号の６４ビットのそれぞれに対応するビット位置が得られる。

【００１５】また、上記演算処理部１０ｂは多段式であり、６４ビットの初期転値後の出力の上位側３２ビットを入力信号Ｌ０として、その下位側の３２ビットを入力信号Ｒ０として受け、これらの信号Ｌ０，Ｒ０に対して演算処理（単なる論理演算のならず、置き換え等その他の処理をも含む）を施す第１の演算処理器１０ｂ１と、その前段の演算器１０ｂｉ（ｉ＝１～１５）からの出力に対して、演算処理を施す第２～第１６の演算器１０ｂｉ＋１（ｉ＋１＝２～１６）とから構成される。

【００１６】ここで、上記第１の演算器１０ｂ１は、上記初期転値出力の下位側３２ビットである入力信号Ｒ０に対して暗号鍵Ｋ１に基づく演算処理を施して関数演算出力ｆ（Ｒ０，Ｋ１）を出力する関数演算回路１１ｂ１と、該関数演算出力ｆ（Ｒ０，Ｋ１）と上記初期転値出力の上位側３２ビットである入力信号Ｌ０との排他的論理和を求める（計算する）排他的論理和回路（ＥＸＯＲ回路）１２ｂ１からなり、上記入力信号Ｒ０をそのまま上位側３２ビット信号Ｌ１として、上記排他的論理和回路からの出力を下位側３２ビット信号Ｒ１として後段の演算器１０ｂ２へ出力する。

【００１７】上記第２～第１６の演算器１０ｂ２～１０ｂ１６は同様に、それぞれ関数演算回路１１ｂ２～１１ｂ１６と排他的論理和回路（ＥＸＯＲ回路）１２ｂ２～１２ｂ１６からなり、各前段の演算器１０ｂ１～１０ｂ１５からの下位側３２ビット信号Ｒ１～Ｒ１５をそのまま各上位側３２ビット側Ｌ２～Ｌ１６として、各ＥＸＯＲ回路１２ｂ１～１２ｂ１５からの出力を各下位側３２ビット信号Ｒ２～Ｒ１６としてその後段側に出力するようになっている。

【００１８】また、第２～第１６の演算器１０ｂ２～１０ｂ１６における関数演算回路１１ｂｉ（ｉ＝２～１６）は、各前段の演算器１０ｂｉ－１（ｉ－１＝１～１５）のＥＸＯＲ回路１２ｂｉ－１（ｉ－１＝１～１５）からの３２ビット出力に、各暗号鍵Ｋｉ（ｉ＝２～１６）に基づく（を使用する）関数演算処理ｆ（Ｒｉ，Ｋ

ｉ＋１）（ｉ＝１～１５）を施して、その演算結果を出力する。

【００１９】また、上記第２～第１６の演算器１０ｂ２～１０ｂ１６におけるＥＸＯＲ回路１２ｂ２～１２ｂ１６は、各その関数演算出力ｆ（Ｒ１，Ｋ２）～ｆ（Ｒ１５、Ｋ１６）と、前段の演算器から出力される各上位側３２ビット信号Ｌ１～Ｌ１５との排他的論理和を求める。

【００２０】ここで、上記関数演算における変換処理を一般的に示すと、第ｎ番目の演算器における変換処理の対称となる入力を（Ｌｎ－１、Ｒｎ－１）、この変換処理に用いられる鍵入力をＫｎとすると、その演算処理結果（Ｌｎ，Ｒｎ）は

Ｌｎ＝Ｒｎ－１

Ｒｎ＝Ｌｎ－１　ｅｏｒ　ｆ（Ｒｎ－１，Ｋｎ）

で与えられる。ここで、「ｅｏｒ」は排他的論理和を示している。また、ｆ（Ｒ，Ｋ）は、４８ビットの情報Ｋに依存して（適切に使用して）３２ビット情報Ｒを変換した、そして３２ビットからなる変換結果（あるいは変換器）を示している。なお、この関数は前掲の岡本栄治著「暗号理論入門」３８～４１ページ記載の非線形関数である。

【００２１】さらに、最終転値処理部１０ｃでは、図５（ｂ）に示す転値データに基づく最終転値処理として、前記演算処理器１０ｂ１６からの上位側３２ビット信号Ｌ１６及び下位側３２ビット信号Ｒ１６からなる６４ビットの本来的な演算処理を終了したデータ信号のビット値の配列を変える。

【００２２】この図５（ｂ）に示す最終転値処理ＩＰ－１用の逆転値データは、上記初期転値データと同じく、６４ビットからなる入力信号の各ビット桁のデータ値が、６４ビットからなる最終転値後の出力データの何ビット目のデータ値になるかを示している。

【００２３】次に、多少冗長（繰り返し）とはなるが、この装置の動作（暗号処理）について説明する。ＤＥＳ方式の暗号処理では、まず、暗号化回路１０に６４ビット平文Ｈｉｎが入力されると、初期転値処理部１０ａがこの入力された平文に対して一定の初期転値処理ＩＰを施す。この初期転値処理を施された各６４ビットからなる信号は、演算処理部１０ｂにおける１６段の演算器１０ｂ１～１０ｂ１６にて変換（暗号化）が施される。

【００２４】すなわち、６４ビットの初期転値された信号が上記演算処理部に入力されると、まず第１の演算器１０ｂ１にて、その下側３２ビット信号Ｒ０に対して、暗号鍵Ｋ１を用いた関数演算処理が施され、さらに、その演算出力ｆ（Ｒ０，Ｋ１）と、上記転値信号の上位側３２ビット信号Ｌ０との排他的論理和がＥＸＯＲ回路１２ｂ１にて求められる。しかる後、この演算器１０ｂ１からは、後段の第２の演算器１０ｂ２へこの排他的論理和が下位側３２ビットの信号Ｒ１として出力される。また、初期転値されて入力された信号の下位側３２ビット信号Ｒ０が、後段の第２の演算器１０ｂ２へその上位側３２ビットの信号Ｌ１として出力される。

【００２５】次に、第２の演算器１０ｂ２では、入力された下位側３２ビットの信号Ｒ１に対して、暗号鍵Ｋ２を用いた関数演算処理が施され、更にその演算処理の出力ｆ（Ｒ１，Ｋ２）と、第１の演算器から入力された上位側３２ビットの信号Ｌ１との排他的論理和がＥＸＯＲ回路１２ｂ２にて求めらる。そして、この演算器１０ｂ２からは、排他的論理和が下位側３２ビットの信号Ｒ２として、また第１の演算器から入力された下位側３２ビットの信号Ｒ１が上位側３２ビットの信号Ｌ２として後の第３の演算器へ出力される。

【００２６】以下、後段の各演算器１０ｂ３～１０ｂ１６では、それぞれ入力される上位側３２ビットの信号Ｌ２～Ｌ１５及び下位側３２ビットの信号Ｒ２～Ｒ１５に対して上述と同様な処理が、各暗号鍵Ｋ３～Ｋ１６を用いて行われる。そして、第１６の演算器１０ｂ１６からの上位側３２ビットの信号Ｌ１６は下位側３２ビットして、同じく下位側３２ビットの信号Ｒ１６が上位側３２ビットとして最終転値処理部１０ｃに入力される。

【００２７】この最終転値処理部１０ｃでは、初期転値処理ＩＰと同じく、６４ビット信号のそれぞれのビットについて最終転値処理ＩＰ－１を施す。この最終転値処理ＩＰ－１による変換を終えることにより、６４ビットからなる平文Ｈｉｎに対する６４ビットからなる暗号文Ａｏｕｔが出力される。そして、この暗号文Ａｏｕｔが公開通信網を介してて送信される。一方、この暗号化された文を受信した方では、予め定められた逆の（原則）演算処理を行なって解読することとなる。

【００２８】

【発明が解決しようとする課題】ところで、暗号装置においては、第三者によるデータの盗聴、偽造、改ざん等からデータを確実に保護する（解読されないようにし、また詐称を防止する）ことが要求されているが、最近では暗号の解読装置としてのコンピュータの処理速度の向上、更には暗号解読方法の進歩により、暗号装置の信頼性（解読困難性等）が低下している。

【００２９】その対策として、色々なアルゴリズムを採用して信頼性が向上した暗号装置が開発されているものの、今度はこれと引き換えに、従来の暗号装置との互換性（相互に暗号通信を行なうことの可能性）がなくなってしまう。言い換えると、改良されたアルゴリズムを採用した暗号装置に従来の暗号装置との互換性を持たせようとすると、従来の暗号装置との互換性維持のために新しく回路を追加して設ける必要があり、ひいては装置全体の回路規模が大きくなり、開発期間、コストの増大につながる。

【００３０】このため、信頼性が向上するとともに、従来の暗号装置との間で互換性を保持しえる暗号装置の開

発が望まれていた。

【００３１】

【課題を解決するための手段】本発明は、以上の目的を達成するためなされたものあり、鍵を種々の手段により変更等するものである。具体的には以下のごとくしている。

【００３２】請求項１記載の発明においては、送信すべきデータたる平文を所定のビット数からなるデータに分割し、得られた個々の分割データを順次暗号化して送信する暗号装置において、上記個々の分割データを暗号化するために暗号鍵を使用して演算処理を行うデータ処理手段と、該データ処理手段が使用する暗号鍵を、予め保持している暗号鍵作成用のデータやプログラムあるいは別途の情報を基に作り出す暗号鍵処理手段とを有していることを特徴としている。

【００３３】上記構成により、以下の作用がなされる。データ処理手段は、上記個々の分割データを暗号化するために少なくも第三者には秘密にされている（信頼のおける第三者を介する場合がある）暗号鍵を使用して、排他的論理和、その他各種の演算処理を行う。暗号鍵処理手段は、データ処理手段が使用する暗号鍵を、予め保持している暗号鍵作成用のデータ、例えば共有鍵や送信側のみが秘密に保持する秘密鍵（本来の「鍵」）や秘密鍵の特定の桁値のみを取り出す等のプログラムあるいは時計やカレンダーからの日時等別途の情報を基に秘密鍵を使用する等して作り出す。

【００３４】そして、これを受信した側では、予めの取決めや共有鍵等を使用して復号することとなる。さらにこれらのため、送信及び受信装置には必要なプログラムやデータを書き込んだＩＣカード等を装着可能となっており、送信（受信）装置のＣＰＵがこのＩＣカードから読み込んだデータ等を基に暗号化（復号）するようになっていたりする。ただし、読み込んだデータ等をもとに所定の動作をなすのは、ワープロのプリンターにおける特殊な字体での印刷等日常の機器にも広く採用されている技術であるため、この説明は省略する。

【００３５】請求項２記載の発明においては、前記データ処理手段は、前記暗号鍵処理手段から入力された暗号鍵を基に、上記個々の分割データに順に演算処理をする鍵基演算小手段を有していることを特徴としている。

【００３６】上記構成により、以下の作用がなされる。鍵基演算小手段は、前記暗号鍵処理手段から入力された暗号鍵を基に、その暗号鍵との排他的論理和をとる等して上記個々の分割データに演算処理をする。

【００３７】請求項３記載の発明においては、前記データ処理手段は、入力された個々の分割データに多段に演算処理を施すが、この際先の段へ入力されたデータの半数が続行する後の段へその半数分の入力データとしてビット桁の位置のみを換えて入力され、先の段から出力されたデータの半数が後の段へその残り半数分の入力データとして入力される演算を行なうインボリューション演算モード小手段を有していることを特徴としている。

【００３８】上記構成により、以下の作用がなされる。データ処理手段内のインボリューション演算モード小手段は、入力された個々の分割データに多段に演算処理を施すが、受信側での解読がハード的に便利なように、この際先の段へ入力されたデータの半数が続行する後の段へその半数分の入力データとして（少なくともその一部は）ビット桁の位置のみを換えてそのままの値で入力され、先の段から処理を施して出力されたデータの半数が続行する後の段へその残り半数分の入力データとして入力されるインボリューション演算を行なう。

【００３９】請求項４記載の発明においては、前記鍵基演算小手段は、各段の演算処理毎に、前記暗号鍵処理手段から異なる暗号鍵を入力されて演算処理をする相違暗号鍵使用小小手段を有していることを特徴としている。

【００４０】上記構成により、以下の作用がなされる。鍵基演算小手段内の相違暗号鍵使用小小手段は、各段での演算処理毎に、前記暗号鍵処理手段から異なる値の暗号鍵を入力され、この異なる値の鍵を使用して演算処理をする。

【００４１】請求項５記載の発明においては、前記暗号鍵処理手段は、外部からのデータに基づいて、前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する外部値依存出力小手段を有していることを特徴としている。

【００４２】上記構成により、以下の作用がなされる。鍵基演算小手段内の外部値依存出力小手段は、外部から入力される日、時、分秒、送信先の番号やそこへの送信回数等のデータに基づいて、前記データ処理手段に出力する暗号鍵を上記各分割データ毎に、例えば秘密鍵から循環的に幾つかの桁の値を取り出す等して、変更する。

【００４３】従って、受信側では、暗号化された文の送信先を局から送られてくる送信側の回線番号等を利用して確認後、必要に応じて内蔵する時計、カレンダー、メモリー等から復号用データを読み出し、更にこのもとで復号することとなる。

【００４４】請求項６記載の発明においては、受信側と予め取り決めた乱数表やプログラム等の乱数発生手段を有し、更に前記暗号鍵処理手段は、前記乱数発生手段の発生させる乱数にもとづいて、前記データ処理手段に出力する暗号鍵を上記分割データ毎に変更する乱数依存出力小手段を有していることを特徴としている。

【００４５】上記構成により、以下の作用がなされる。乱数依存出力小手段は、前記乱数発生手段の発生させる乱数にもとづいて、前記データ処理手段、そして特に鍵基演算小手段に出力する暗号鍵を上記分割データ毎に変更する。

【００４６】したがって、受信側では別途あるいは同時に送信されてきた乱数についてのデータをもとに乱数を

計算し、復号をなすこととなる。具体的には、例えば、送信側は暗号化に使用した乱数の下位桁の数値を併せて送信し、受信側では所定の手順で乱数を発生させ、何回目かに下位桁の数値が一致した乱数を使用して復号する等である。

【００４７】請求項７記載の発明においては、前記暗号鍵処理手段は、入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更するビット依存出力小手段を有していることを特徴としている

【００４８】上記構成により、以下の作用がなされる。前記暗号鍵処理手段内のビット依存出力小手段は、入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する。具体的には、例えば最初の桁のビット値が１ならばこれに応じて、発生させる暗号鍵を１つずらす。（従って、解読のためにはその変更に応じての何らかの情報も同時若しくは別途送信されたり、別途送信者と受信者とで取り決められていたりすることとなる。）

【００４９】請求項８記載の発明においては、前記暗号鍵処理手段は、前入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する前ビット依存出力小手段を有していることを特徴としている。

【００５０】上記構成により、以下の作用がなされる。前記暗号鍵処理手段内の前ビット依存出力小手段は、前入力データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する。

【００５１】請求項９記載の発明においては、前記暗号鍵処理手段は、前暗号データの全ビット又は特定の数ビットにもとづいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する前暗号データ依存鍵変更小手段を有していることを特徴としている。

【００５２】上記構成により、以下の作用がなされる。暗号鍵処理手段内の前暗号データ依存鍵変更小手段は、前暗号データの全ビット又は特定の数ビットにもとずいて前記データ処理手段に出力する暗号鍵を上記各分割データ毎に変更する。（例えば、先頭のビットが１ならば、発生させる暗号鍵を１つだけ循環させて使用し、しかも各分割データのブロック番号毎にこの１を０に交互に変更する。）

【００５３】

【発明の実施の形態】以下、本発明をその実施の形態にもとずいて説明する。図１は、本発明に係わる暗号装置の実施の形態の構成図である。本図において、１００は本暗号装置そのもの（全体）である。また１０１は、入力データを保持する入力データラッチ回路である。１０２は、暗号処理回数制御回路である。１０３は、暗号処理回数制御回路から出力されるセレクト信号に基づいて、入力データラッチ回路からの出力及び暗号処理回数制御からの出力のうちいずれか一方を選択するセレクタ回路である。１０４は、暗号鍵処理回路である。１０５は、暗号鍵処理回路から出力される暗号鍵と、セレクタ回路からの出力信号とを入力されて所定の演算処理を行なう演算処理回路である。１０６は、演算処理回路の演算結果を保持する出力データラッチ回路である。

【００５４】以上の他、送受信先の回線番号毎の送受信回数の記憶手段、送受信者間の取決め（言わば、プロトコル）の記憶手段、暗号化や復号のみならず送受信を統一して制御するＣＰＵ、モデムやアンテナ等を有しているのは勿論である。但し、これらは、いわば自明であるため、わざわざの図示は省略する。

【００５５】さらに、例えば、送受信先の回線番号毎に送受信回数を記憶することや本文の送受信に先立って送受信者間の取決め（プロトコル）に従って必要なデータを交換すること等は、送信記録の自動出力、Ｇ３かＧ４かの確認等ファクシミリにも採用されている技術である。このため、これら作用発揮のためのハードやソフトの説明も省略する。

【００５６】上記演算処理回路は、図２に示すように、６４ビットのセレクタ回路からの出力のうち、下位側３２ビットの信号ＬＳＢに対して暗号鍵処理回路から出力される暗号鍵に基づいて関数ｆにより関数演算処理を施す関数演算回路２０３と、この関数演算回路からの出力と上記セレクタ回路から出力される信号のうち上位側３２ビットの信号ＭＳＢとの排他的論理和をとるＸＯＲ回路２０２とを有し、このＸＯＲ回路から出力される３２ビットのデータと上記下位側３２ビットの信号ＬＳＢとからなる６４ビットの演算処理結果を出力し、さらに１６回の演算処理が終了すると、その結果を出力データ回路に出力する構成となっている。

【００５７】ここで、上記関数ｆは、従来技術と同じく前掲の岡本著「暗号理論入門」３８、３９ページに記載されている非線形関数ｆと同じものである。上記暗号鍵処理回路は、図３に示すように、別途図示しない外部から入力された暗号鍵データを使用して暗号鍵処理関数（回路）３０１内で暗号鍵Ｋ１からＫ１６を作成し、これらを各段での処理の際順に出力する。そしてこの出力たる暗号鍵Ｋ１からＫ１６は、タイミング用クロック信号等の外部入力によって暗号鍵セレクタ回路３０２内でセレクトされ、該当する段での処理に使用されるべく暗号鍵処理回路からタイミングよく出力され、演算処理回路へ入力される。

【００５８】暗号処理回数制御回路は、図４に示すように、セレクタ信号が上記の演算処理回数にて処理される度にカウント値がインクリメントし、かつ該カウント値が１６回になると次の分割データを暗号化するべくリセットされるカウンター回路４０２と、演算処理回数を格納する演算処理回数格納部４０１と、該両回路の出力を

比較し、その比較結果に応じてセレクタ信号を出力するコンパレータ４０３とからなっている。そして勿論、カウント値が１６になると、セレクタ回路に次の平分ブロックを演算処理する旨の指示信号を出力する。

【００５９】次に、以上の構成の暗号装置の作用について説明する。今、１２８ビットの平文を暗号化するものとして、その内容を説明する。まず、１２８ビットの平文が、それぞれの６４ビットの２つの平文ブロック、つまり６４ビットの第１の平文ブロックと、第２の平文ブロックに分割される。

【００６０】次に、この分割された各平文ブロックの暗号化が本暗号装置１００により順に行われる。すなわち、この第１、第２の平文ブロックは、順に入力データラッチ回路１０１に入力され、この入力データラッチ回路にて平文ブロックの暗号化処理が終了するまで保持される。

【００６１】入力データラッチ回路から先に出力された第１の平文ブロックのビットデータは、セレクタ回路に入力される。このセレクタ回路は、第１の平文ブロックのビットデータの入力に伴い、暗号処理回数制御回路の演算処理回数格納部に格納されている予め決められた暗号処理回数（１６回）から最初の１回を引いた１５回に相当する信号を受け、これに基づいて演算処理回路からの出力と、入力データラッチ回路からの出力のうち後者を選択し、これを演算処理回路に出力する。そして、これにより第１の平文ブロックのビットデータに対する第一段の処理がなされることとなる。

【００６２】このとき、演算処理回路への第１回目の入力は、入力データラッチ回路からの出力値である。また、暗号鍵処理回路では、各段１６回の暗号処理に使用される４８ビットの暗号鍵Ｋ１～Ｋ１６が、暗号鍵データ入力により作られる。そして、これらの暗号鍵は、演算処理回路に逐次タイミングよく入力され、演算処理回路での第１回から第１６回目までの処理にそれぞれ対応した固有の暗号鍵が使用されることとなる。

【００６３】なお、各段での演算処理に使用される暗号鍵は、暗号鍵処理回路へその外部から入力される別途の指示データにて、その出力順序や桁等を変更、交換することが可能である。但し、このためのハードやソフトそのものは特に困難とは思われないので、その説明は省略する。更にまた、当然受信側でもこのためのハードやソフトのみならず暗号化に使用されたデータの知得が必要であるが、これらについては特に困難とは思われないので、その説明は省略する。

【００６４】そして、暗号処理回数制御回路であらかじめ格納されている回数だけのインボリュウション処理を行った後、演算処理回路から暗号化されたが出力データラッチ回路に出力される。（そして、ここで暗号化された第１の平文ブロックのビットデータが出力されるまで保持されることとなる。）

【００６５】これと同時に、入力データラッチ回路から次の第２の平文ブロックのビットデータがセレクタ回路に入力され、前の平文ブロックと同様の演算処理が行われ、これが終了すると、出力データラッチ回路に出力される。なおこの際、暗号鍵処理回路は、別途のデータ入力のもと、先の第１の平文ブロックと第２の平文ブロックとで各段で使用する鍵の順番を入れ換える等しても良いのは勿論である。

【００６６】以上の演算処理が終了すると、出力データラッチ回路に保持されている二つの暗号化された平文ブロックからなるビットデータは暗号化された送信文として、受信側へ公開通信網を介して送信されることとなる。

【００６７】以上、本発明をその実施の形態にもとずいて説明してきたが、本発明はなにも以上の実施の形態に限定されないのは勿論である。即ち、例えば以下の様にしていてもよい。

① 本発明の１の特定事項（構成要素）を、製造等の都合で物理的に複数のものとしたり、その逆に複数の特定事項を１に合体したりしている。

② 暗号鍵処理回路の暗号鍵セレクタ回路に外部入力を使用せず、これに換えて乱数発生回路で発生させた乱数、平文ブロック、前平文ブロック、前暗号データを入力する様にしている。

【００６８】③ 平文を分割するビットサイズは６４ビットでなく、例えば１２８ビットとしている。さらには、暗号鍵と平文を分割するビットサイズを大きくし、その代わり暗号処理回数を１６回未満としている。

【００６９】④ 外部入力をある値にすることにより、ＤＥＳ暗号装置と同等な機能を有する様にしており、またこのための外部入力をあらかじめＲＯＭに記憶していたり、ＩＣカード等から読込可能としている。

⑤ 装置の暗号アルゴリズムが解読された場合でも、装置そのものを変更することなく、暗号アルゴリズムを変更することによりデータの秘密性を保持しえるべく、演算処理回路で使用する暗号鍵を平文ブロック毎に変更可能している。

【００７０】⑥ 各段の暗号鍵の順序を変更可能として、ＤＥＳ暗号装置と異なるものとしている。あるいは、転置処理等他の暗号化手段を併用している。

⑦ 演算処理回路がインボリューション演算であるのを利用して、復号装置に転用している。

⑧ 暗号処理回数を同一相手先への送信回数に応じて変更する等している。

【００７１】⑨ ＩＣカード等のプログラムやデータ記憶手段を装着可能、しかも装着したＩＣカード等から読み込んだデータにもとづいて本発明の作用をなすようにしている。またこれにより、ＩＣカード等を交換するだけで本発明の相異なる各種の作用をなしうるようにしている。

13

【００７２】

【発明の効果】以上説明してきたように、本発明によれば、各演算処理毎の暗号鍵を外部より制御（変更）可能にしたため、暗号アルゴリズムを外部から簡単に変更することができる。このため、第三者によるデータの盗聴、改ざん、解読、詐称等への耐性が向上し、また万一第三者によりアルゴリズムが解読された場合でも、その解読手段がどのようなものであれともかくハードの変更を行うことなく、暗号アルゴリズムの変更ですなわちソフトで対応することが可能となる。

【００７３】また、データ処理手段として、所定ビットの暗号鍵を用いて関数データに基づいた演算処理を施す演算処理回路と、選択された暗号鍵を出力する暗号鍵処理回路を備えたので、関数データを既存のＤＥＳ暗号方式に対応したものにすることにより、これらの方式の暗号装置との互換性を有し、しかもより解読困難な暗号装置としえる。なお、暗号鍵処理手段で暗号鍵を制御しえるため、より解読等が困難な暗号装置となっているのは勿論である。

【００７４】また、データ処理手段を、その出力データを入力データとする第２の演算処理を行った場合に、最初の入力データと出力データとが同じ値になるインボリューション演算モードとしたので、暗号回路と復号回路を同一にする事が可能となる。また、複数回のデータ処理を行う際、使用する暗号鍵を変更するため、既存のＤＥＳ暗号方式に対応したものにすることが可能となり、これらとの互換性が失われず、しかもより解読困難な装置となっている。

【００７５】また、複数回のデータ処理を行う際、使用する暗号鍵を各段の処理毎に外部入力等により変更するため、既存のＤＥＳ暗号方式の装置と互換性を有しつつ、より解読困難な装置となっている。また、複数回のデータ処理を行う際、使用する暗号鍵を各段の処理毎に外部の回路で発生させた乱数により変更するため、既存のＤＥＳ暗号方式の装置と互換性を有しつつ、より解読困難な装置となっている。

【００７６】また、複数回のデータ処理を行う際、使用する暗号鍵を、各段の処理毎に外部から入力されるデータにより変更するため、既存のＤＥＳ暗号方式の装置と互換性を有しつつ、より解読困難な装置となっている。また、複数回のデータ処理を行う際、使用する暗号鍵を、各処理毎に外部からの前入力データにより変更するため、既存のＤＥＳ暗号方式の装置と互換性を有しつ

14

つ、より解読困難な装置となっている。

【００７７】また、複数回のデータ処理を行う際、使用する暗号鍵を、各段の処理毎に前の暗号データにより変更するため、既存のＤＥＳ暗号方式の装置と互換性を有しつつ、より解読困難な装置となっている。

【図面の簡単な説明】

【図１】本発明の暗号装置の実施の形態の全体構成図である。

【図２】上記暗号装置の演算処理回路の構成図である。

【図３】上記暗号装置の暗号鍵処理回路の構成図である。

【図４】上記暗号装置の暗号処理回数制御回路の構成図である。

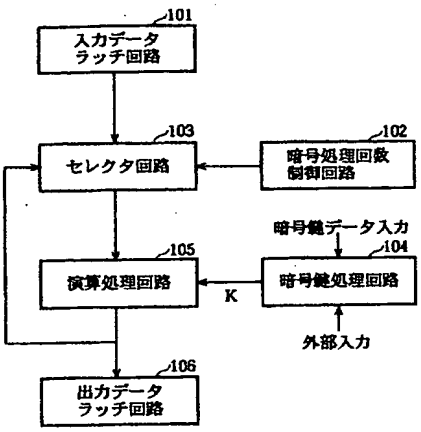
【図５】従来のＤＥＳ暗号方式の転値回路における処理の内容を、表にて示した図である。（本図の（ａ）に初期転値回路の処理の内容を、（ｂ）に最終転値回路の処理の内容を示す。）

【図６】従来のＤＥＳ暗号方式の暗号化回路の構成図である。

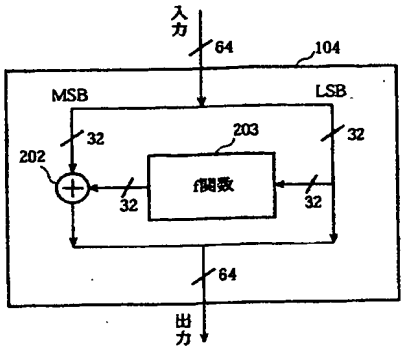
【符号の説明】

１００	暗号装置
１０１	入力データラッチ回路
１０２	セレクタ回路
１０３	暗号処理回数制御回路
１０４	演算処理回路
１０５	暗号鍵処理回路
１０６	出力データラッチ回路
２０２	排他的論理和回路
２０３	関数演算回路
３０１	暗号鍵処理回路
３０２	セレクタ回路
４０１	暗号処理回数格納部
４０２	カウンター回路
４０３	コンパレータ
１０ａ	初期転値処理部
１０ｃ	最終転値処理部
Ｋ１	第１の暗号鍵
Ｋ２	第２の暗号鍵
Ｋ１６	第１６の暗号鍵
１０ｂ１，１０ｂ２，１０ｂ１６	演算器
１１ｂ１，１１ｂ２，１１ｂ１６	関数演算回路
１２ｂ１，１２ｂ２，１２ｂ１６	排他的論理和回路

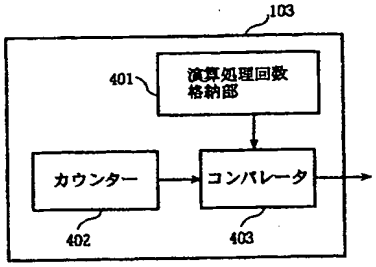
【図１】



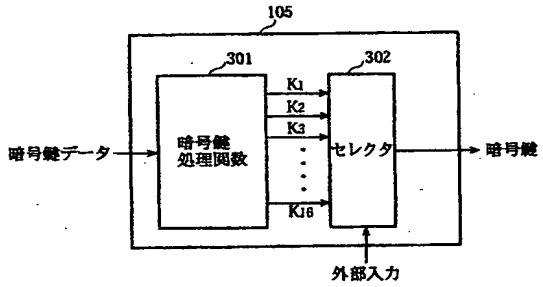
【図２】



【図４】



【図３】



【図５】

(a)

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

(b)

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

【図６】